REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)* 03-05-2010	**2. REPORT TYPE** FINAL	**3. DATES COVERED** *(From - To)*
4. TITLE AND SUBTITLE **Fleet Cyber Command/TENTH Fleet: Enabling Cyber Unity of Effort**		**5a. CONTRACT NUMBER** **5b. GRANT NUMBER** **5c. PROGRAM ELEMENT NUMBER**
6. AUTHOR(S) **LCDR Joseph E. Sisson, USN**		**5d. PROJECT NUMBER** **5e. TASK NUMBER** **5f. WORK UNIT NUMBER**
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Joint Military Operations Department Naval War College 686 Cushing Road Newport, RI 02841-1207		**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)		**10. SPONSOR/MONITOR'S ACRONYM(S)** **11. SPONSOR/MONITOR'S REPORT NUMBER(S)**

12. DISTRIBUTION / AVAILABILITY STATEMENT
DISTRIBUTION STATEMENT A. Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

The rapid advance of technology and the world's dependence on the internet and telecommunications for personal, business, and government activities has provided a new domain--cyber--to be exploited and attacked by U.S. adversaries. In order to counter this growing threat a transformation within the U.S. Department of Defense has begun with the establishment of U.S. Cyber Command (CYBERCOM) and the Navy cyber component, Fleet Cyber Command/TENTH Fleet. Fleet Cyber Command/TENTH Fleet is an organization that was established to harness the myriad missions currently in Navy doctrine to produce an economy of force and unity of effort across the four fields of information, intelligence, communications and command and control (C^2) to create a force capable of conducting and supporting operations in cyberspace. Fleet Cyber Command/TENTH Fleet's command organization and relationships will enable it to achieve unity of effort by fusing Navy's cyber, information operations, cryptologic and space capabilities under the command and control of a single commander.

15. SUBJECT TERMS
Cyber; Cyberspace; TENTH Fleet; Fleet Cyber Command; Command Organization; Unity of Effort; Unity of Command

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Department
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		**26**	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3414

NAVAL WAR COLLEGE
Newport, R.I.

Fleet Cyber Command/TENTH Fleet: Enabling Cyber Unity of Effort

by

Joseph E. Sisson

Lieutenant Commander / U.S. Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____________________

03 May 2010

Contents

List of Illustrations

Abstract

The rapid advance of technology and the world's dependence on the internet and telecommunications for personal, business, and government activities has provided a new domain--cyber--to be exploited and attacked by U.S. adversaries. In order to counter this growing threat a transformation within the U.S. Department of Defense has begun with the establishment of U.S. Cyber Command (CYBERCOM) and the Navy cyber component, Fleet Cyber Command/TENTH Fleet. Fleet Cyber Command/TENTH Fleet is an organization that was established to harness the myriad missions currently in Navy doctrine to produce an economy of force and unity of effort across the four fields of information, intelligence, communications and command and control (C^2) to create a force capable of conducting and supporting operations in cyberspace. Fleet Cyber Command/TENTH Fleet's command organization and relationships will enable it to achieve unity of effort by fusing Navy's cyber, information operations, cryptologic and space capabilities under the command and control of a single commander.

The Challenge: Achieving Unity of Effort

"... separate ground, sea and air warfare is gone forever. If ever again we should be involved in war, we will fight it in all elements, with all services, as one single concentrated effort. Peacetime preparatory and organizational activity must conform to this fact. Strategic and tactical planning must be completely unified, combat forces organized into unified commands, each equipped with the most efficient weapons systems that science can develop, singly led and prepared to fight as one, regardless of service."[1]

President Dwight D. Eisenhower

Introduction

The rapid advance of technology and the world's dependence on the internet and telecommunications for personal, business, and government activities has provided a new domain--cyber--to be exploited and attacked by U.S. adversaries. President Obama addressed the importance of protecting the nation's cyber domain when he stated, "our technological advantage is a key to America's military dominance. But our defense and military networks are under constant attack. Indeed, in today's world, acts of terror could come not only from a few extremists in suicide vests but from a few key strokes on the computer -- a weapon of mass disruption."[2] In order to counter this growing threat a transformation within the U.S. Department of Defense has begun with the establishment of U.S. Cyber Command (CYBERCOM) and the Navy cyber component, Fleet Cyber Command/TENTH Fleet.[3] Fleet Cyber Command/TENTH Fleet's command organization and relationships will enable it to achieve unity of effort by fusing Navy's cyber, information operations, cryptologic and space capabilities under the command and control of a single commander. The organizational relationships and the process of

[1] Dwight D. Eisenhower, Presidential Message, *Public Papers of the Presidents, Dwight D. Eisenhower, 03 April 1958, The American Presidency Project:* Santa Barbara, CA., http://www.presidency.ucsb.edu/ws/?pid=11340 (accessed 23 March 2010).

[2] http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (accessed 03 February 2010).

[3] William M. Gates, Secretary of Defense, Department of Defense, to Secretaries of the Military Departments, memorandum, 23 June 2009.

synchronizing and sequencing actions, whether defensive or offensive in nature, amongst the many entities conducting operations across the cyber domain are instrumental in determining whether the United States will have an effective cyber capability.[4] A cohesive, agile and resilient command organization is essential to enabling joint cyber operations in the 21st Century. In order to create and maintain an effective joint cyberspace capability at the operational level unity of effort must be achieved between the organizations tasked with cyberspace missions.

This paper will focus on an analysis of the command organization of Fleet Cyber Command/TENTH Fleet to support the thesis that the establishment of this new organization empowers, not impedes, the joint force's cyber unity of effort. First, in order to frame the discussion, this paper will describe what constitutes cyberspace and how this warfare domain differs from the traditional land, air and sea domains in terms of Operational Factors time, space and force. Also, it will provide context to the cyber threat posed to the United States. Second, this paper will analyze the current Fleet Cyber Command/TENTH Fleet command organization, missions and relationships and discuss how unity of effort can be achieved through unity of command and organizational command and control (C^2). Third, this paper will consider a counter-argument to the thesis that Fleet Cyber Command/TENTH fleet will fail to achieve unity of effort by violating a basic Operational Command Organization tenant--simplicity.[5] Finally, based on the analysis of the command organization and relationships this paper will present three recommendations to aid the achievement and maintenance of unity of effort.

[4] Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (2007; repr., Newport, RI: Naval War College, 2009), VIII-7.
[5] Ibid, VIII-13.

Framing the Discussion: What does "Cyberspace" Mean?

Cyberspace and information environment are terms sometimes used interchangeably, although they have distinctly separate meanings. Cyberspace is a global domain within the information environment consisting of networks of information technology (IT) infrastructures, including the Internet, telecommunications networks, and computer systems.[6] Effectively, this translates to the hardware and networks that store and transport information. The information environment is the aggregate of all people, organizations, and systems that collect, process, disseminate, or act on information.[7] A clear understanding of what cyberspace is will help the reader visualize a "digital sea" that exists within the warfare domain with physical boundaries of IT hardware.

Today's domain of operations in cyberspace evolved from Command and Control Warfare (C2W) as defined by the Chairman of the Joint Chiefs (CJCS) Memorandum of Policy (MOP) 30 in 1993:

> The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW) and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade or destroy adversary C2 capabilities, while protecting friendly capabilities against such actions. Command and Control Warfare applies across the operational continuum and all levels of conflict.[8]

As technology evolved, and the proliferation of networked communications exploded around the world, cyberspace became a recognized warfare domain along with land,

[6] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, as amended through 31 October 2009), 139.

[7] Ibid, 260.

[8] Chairman, U.S. Joint Chiefs of Staff, Memorandum of Policy (MOP) 30, *Command and Control Warfare* (Washington, DC: 1993), 3.

air, maritime and space as outlined in the National Military Strategy for Cyberspace Operations.[9] This warfare domain designation was a result of operational forces having the ability to conduct the six Operational Functions of warfare entirely within cyberspace: Maneuver being accomplished by freedom of movement and action across the information environment; Fires conducted by computer network attack (CNA) and electronic warfare (EW); Protection of friendly networks and information through computer network defense (CND) actions; Sustainment of networks and communications capabilities by network operations (NETOPS); Intelligence derived from data and information gained via computer network exploitation (CNE) and electronic warfare support (ES); and C^2 by operational commanders exercising authority and direction over assigned forces regardless of factor space. Operations in the cyberspace domain expand the traditional boundaries of warfare from land, air, maritime and space. Consideration toward unity of effort must be given since cyberspace transcends the physical boundaries of the geographical combatant commanders and theater of operations.

The Operational Factor of space for land, maritime and sea warfare is more easily defined that that of cyberspace. Identifying the attributes of factor space in terms of topography, people, distances, positions and shapes is more readily applicable to warfare on land, at sea and in the air. Cyberspace is not limited by physical boundaries and transcends geographical and functional boundaries allowing a commander to potentially control forces from thousands of miles away. However,

[9] Chairman, U.S. Joint Chiefs of Staff, *National Military Strategy for Cyberspace Operations* (Washington D.C.: CJCS, December 2006), 3.

because cyberspace also consists of equipment that is installed at some physical location, a relationship between physical space and cyberspace does exist (Fig. 1).[10]

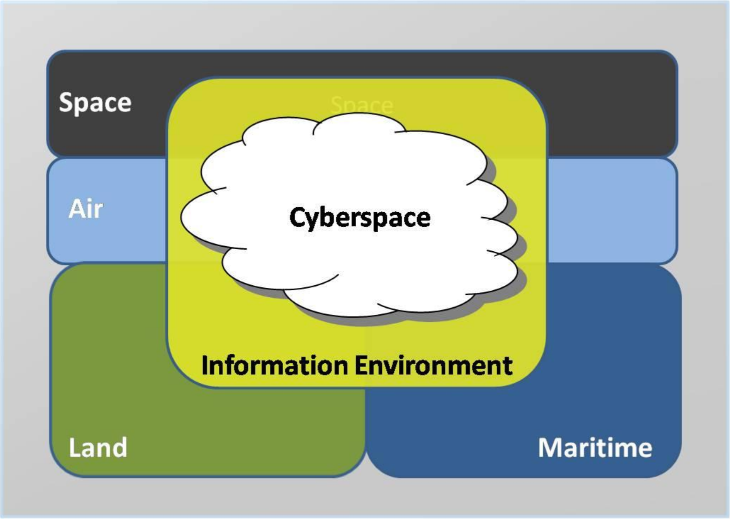


Fig. 1. War Fighting Domain's Relationship with Cyberspace

Time is the Operational Factor most affected by the advent of cyberspace operations. Considered the most precious and critical factor, time cannot be recovered once lost whereas space lost can be regained.[11] Enabling near-simultaneous communications with assigned forces allows a commander to decrease the amount of time required to communicate operational plans, prepare, mobilize and deploy forces. Cyberspace allows a commander to shorten the decision-making cycle while affording greater flexibility during the course of operational warfare.

Of the three Operational Factors, force provides U.S. adversaries the greatest opportunity to gain an advantage and cause harm to U.S. interests. Over a decade ago Director of Central Intelligence, George Tenant, testified to Congress that "countries

[10] Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (2007; repr., Newport, RI: Naval War College, 2009), III-15.
[11] Ibid, III-19.

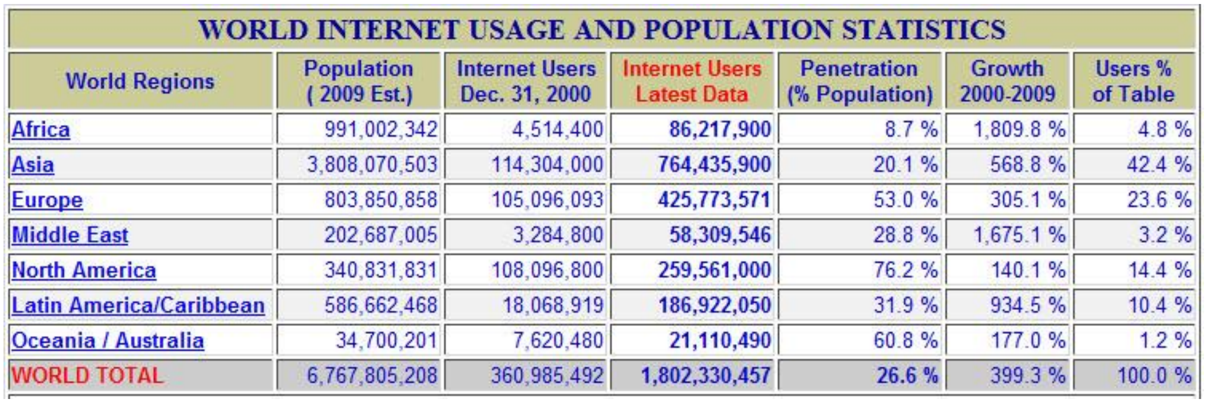
recognize that cyber attacks - possibly launched from outside the US - against civilian computer systems in the US - represent the kind of asymmetric option they will need to "level the playing field" during an armed crisis against the United States."[12] His statement demonstrates that adversaries have the means to conduct cyber attacks against the U.S. across the diplomatic, information, military and economic (DIME) spectrum in order to neutralize any advantage the U.S. may have in combat power.

Vulnerability and Threat

Today the DoD operates more than one thousand five-hundred different computer networks across four thousand military installations around the world.[13] According to the 2010 Quadrennial Defense Review (QDR) report, on any given day, there are as many as seven million DoD computers and telecommunications tools in use in eighty-eight countries providing a staggering number of possible vulnerabilities to our cyberspace and information domain. For context of the global scale of internet usage and growth see figures 2 and 3. Figure 2 provides data on the worldwide usage and growth of the internet while figure 3 depicts a snapshot in time of media usage on a given day (21 April 2010). The exponential growth in global internet penetration and the sheer volume of internet users requires an economy of force in cyber operations that will be enabled by unity of effort between Fleet Cyber Command/TENTH Fleet and CYBERCOM. America's cyberspace and information environment are critical vulnerabilities of the joint force and must be protected.

[12] George Tenet, U.S. CIA Director, quote from prepared remarks made to the Senate Governmental Affairs Committee, https://www.cia.gov/news-information/speeches-testimony/1998/dci_testimony_062498.html, 24 June 1998 (accessed 11 April 2010).

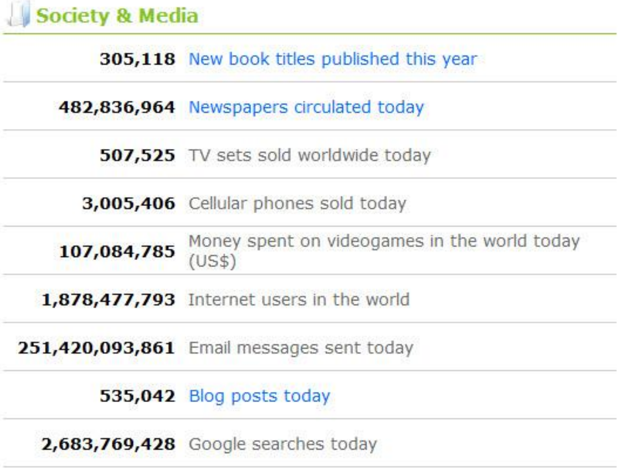
[13] Secretary of Defense, *Quadrennial Defense Review (QDR) Report*, (Washington, DC: The Pentagon, February 2010), 37.



WORLD INTERNET USAGE AND POPULATION STATISTICS

World Regions	Population (2009 Est.)	Internet Users Dec. 31, 2000	Internet Users Latest Data	Penetration (% Population)	Growth 2000-2009	Users % of Table
Africa	991,002,342	4,514,400	**86,217,900**	8.7 %	1,809.8 %	4.8 %
Asia	3,808,070,503	114,304,000	**764,435,900**	20.1 %	568.8 %	42.4 %
Europe	803,850,858	105,096,093	**425,773,571**	53.0 %	305.1 %	23.6 %
Middle East	202,687,005	3,284,800	**58,309,546**	28.8 %	1,675.1 %	3.2 %
North America	340,831,831	108,096,800	**259,561,000**	76.2 %	140.1 %	14.4 %
Latin America/Caribbean	586,662,468	18,068,919	**186,922,050**	31.9 %	934.5 %	10.4 %
Oceania / Australia	34,700,201	7,620,480	**21,110,490**	60.8 %	177.0 %	1.2 %
WORLD TOTAL	6,767,805,208	360,985,492	**1,802,330,457**	**26.6 %**	399.3 %	100.0 %

Fig. 2. World Internet Usage Statistics (http://www.internetworldstats.com/)



Society & Media

305,118	New book titles published this year
482,836,964	Newspapers circulated today
507,525	TV sets sold worldwide today
3,005,406	Cellular phones sold today
107,084,785	Money spent on videogames in the world today (US$)
1,878,477,793	Internet users in the world
251,420,093,861	Email messages sent today
535,042	Blog posts today
2,683,769,428	Google searches today

Fig. 3. Worldwide Media Usage Snapshot--21 April 2010 (http://www.worldometers.info/)

The importance of protecting and defending our country's cyberspace domain is highlighted throughout nearly every national strategy and policy document published over the past decade. The February 2010 Quadrennial Defense Review (QDR), a study conducted every four years by the Department of Defense to confront current and future challenges and serve as a means to develop new policies, capabilities and initiatives, identifies cyberspace as a national security vulnerability. Additionally, the QDR identifies the ability to "operate effectively in cyberspace" as one of the six key missions of the DoD over the next four years.[14] The scale of the Department of Defense's reliance on networked communications makes freedom of operations in cyberspace a de facto critical requirement for joint force operations in the 21st Century.

Command Organization

"It's also very important that TENTH Fleet settle into the relationship that exists between it and the joint headquarters above it and the work they do for STRATCOM (U.S. Strategic Command). Getting those relationships established is key."[15]

Admiral Gary Roughead
Chief of Naval Operations

The overarching Department of Defense organizational structure for commanding and controlling U. S. joint forces is defined by the Unified Command Plan (UCP). The UCP establishes unified and specified commands, assigns missions and functions to those commands, provides for assignment of forces, defines geographic areas of responsibility (AORs), delineates the chain-of-command and establishes command relationships.[16]

In June 2009, Secretary of Defense Robert M. Gates established CYBERCOM as a subordinate unified command of U.S. Strategic Command.[17] CYBERCOM's mission is to plan, synchronize and conduct defense of the Department of Defense information networks as well conduct full spectrum cyberspace operations when directed.[18] In addition to the establishment of CYBERCOM, Secretary Gates ordered the military departments to "identify and provide appropriate component support to USCYBERCOM".[19] As a result, the Chief of Naval Operations (CNO) established Fleet Cyber Command and re-commissioned TENTH

[14] Ibid, 2.

[15] "Navy Must Think Through Approach To Cyber Domain, CNO Says." *Defense Daily*, 05 February 2010, http://www.proquest.com/ (accessed 17 February, 2010).

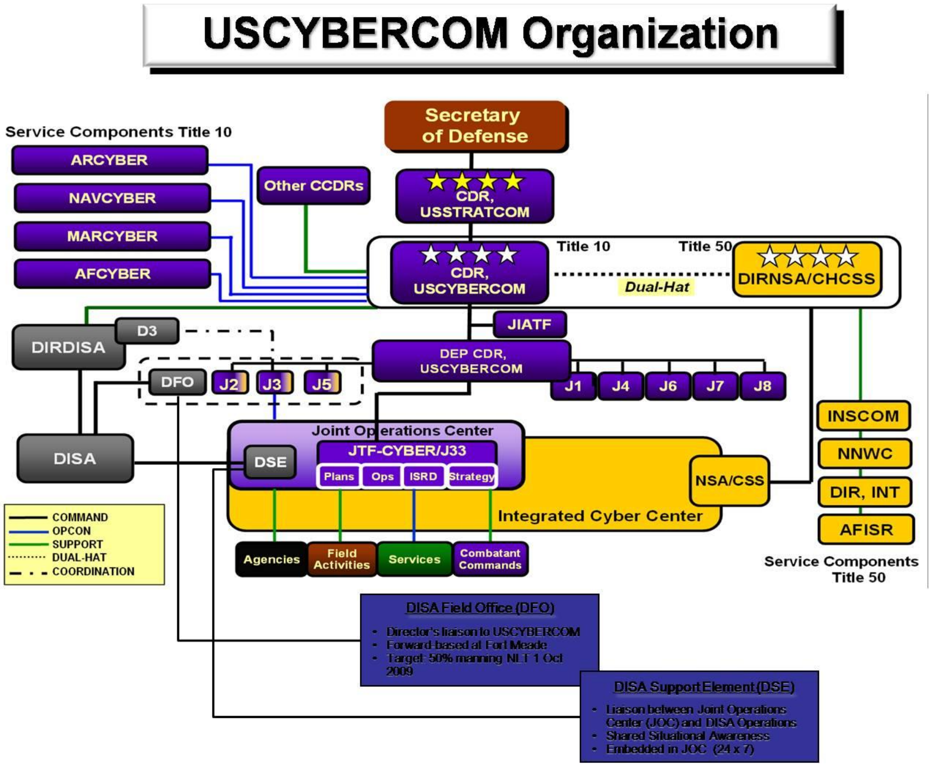
[16] President George W. Bush, *Unified Command Plan*, 17 December 2008, 1.

[17] William M. Gates, Secretary of Defense, Department of Defense, to Secretaries of the Military Departments, memorandum, 23 June 2009.

[18] VADM Barry McCullough. "U.S. Fleet Cyber Command/U.S. TENTH Fleet," Powerpoint, 28 January 2010, Ft. Meade, MD: United States Fleet Cyber Command/10th Fleet, Commander,11.

[19] Ibid

Fleet as the Navy's component to CYBERCOM. The Department of Defense cyber organization is depicted by a standard block organization chart as shown below (Fig. 4).



DISA Field Office (DFO)

- Director's liaison to USCYBERCOM
- Forward-based at Fort Meade
- Target: 50% manning NLT 1 Oct 2009

DISA Support Element (DSE)

- Liaison between Joint Operations Center (JOC) and DISA Operations
- Shared Situational Awareness
- Embedded in JOC (24 x 7)

Fig. 4. USCYBERCOM Organization (http://www.govexec.com/nextgov/)

This graphic illustrates the many organizations tasked with cyber missions with multiple lines of administrative and operational control as well as the relationships of supported and supporting commanders. This command organization for the Department of Defense cyber forces provides the structure for a chain of command and relationships identifying command and support functions. Additionally, these relationships help identify the "...type and degree of authority one commander has over another and the type and degree of support that one commander provides to another."[20]

Fleet Cyber Command/TENTH Fleet is an organization that was established to harness the myriad missions currently in Navy doctrine to produce an economy of force and unity of effort across the four fields of information, intelligence, communications and C^2 (Fig. 5). The goal is to create a force capable of conducting and supporting operations in the cyberspace warfare domain. The Navy's cyber force of Fleet Cyber Command/TENTH Fleet consists of fourteen thousand Sailors and civilians at more than twenty commands dispersed worldwide conducting missions in computer network operations, signals intelligence, naval communications and information operations.[21, 22]

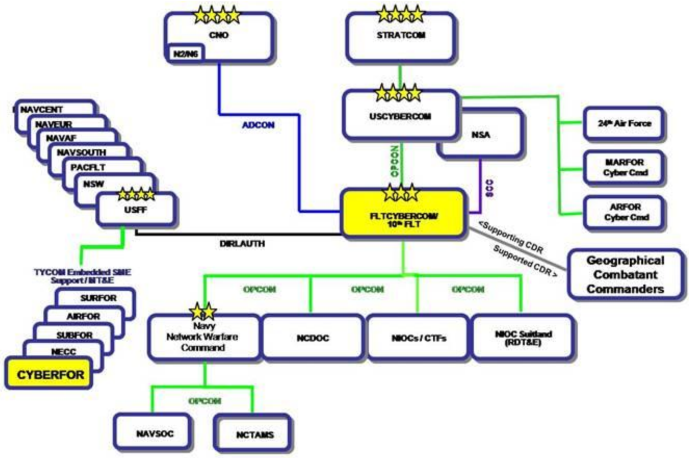


Fig. 5. Fleet Cyber Command/TENTH Fleet Organization

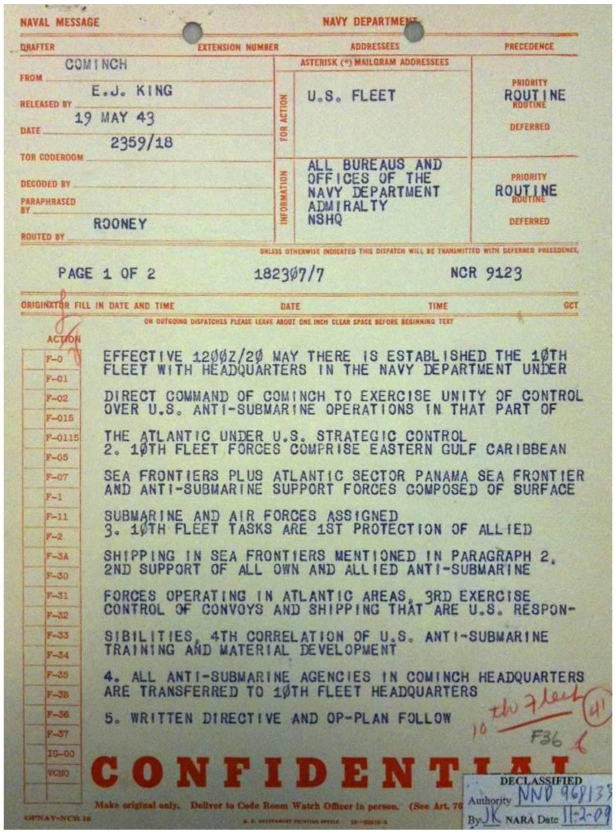
The establishment of Fleet Cyber Command and the concurrent re-commissioning of the TENTH Fleet as the Navy's component to CYBERCOM has been referred to as the

[20] C4I Division, Headquarters U.S. Marine Corps, *Command and Control: A U.S. Marine Corps Concept Paper*, 24 February 1994, pp. 67–69, quoted in Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: U. S. Naval War College, 2009), VIII-7.

[21] Commander, Fleet Cyber Command to Fleet Cyber Command forces, message 291700Z JAN 09, 29 January 2009.

[22] VADM Denby Starling. "CYBERFOR/NETWARCOM Staff Alignment," Powerpoint, 05 February 2010, Norfolk, VA: Navy Cyber Forces/Naval Network Warfare Command, Commander,4.

reemergence of a “fleet-in-being” concept implemented with the original TENTH Fleet during World War II.[23] During World War II, Admiral Ernest J. King, Chief of Naval Operations, established the original TENTH Fleet to “exercise unity of control over U.S. anti-submarine operations in that part of the Atlantic under United States strategic control (Fig. 6).”[24]



NAVAL MESSAGE NAVY DEPARTMENT

DRAFTER EXTENSION NUMBER ADDRESSEES PRECEDENCE

COMINCH
FROM

E.J. KING
RELEASED BY

19 MAY 43
DATE

2359/18
TOR CODEROOM

DECODED BY

PARAPHRASED BY

ROONEY
ROUTED BY

ASTERISK (*) MAILGRAM ADDRESSEES

FOR ACTION: U.S. FLEET

PRIORITY
ROUTINE
ROUTINE
DEFERRED

INFORMATION: ALL BUREAUS AND
OFFICES OF THE
NAVY DEPARTMENT
ADMIRALTY
NSHQ

PRIORITY
ROUTINE
ROUTINE
DEFERRED

UNLESS OTHERWISE INDICATED THIS DISPATCH WILL BE TRANSMITTED WITH DEFERRED PRECEDENCE.

PAGE 1 OF 2 182307/7 NCR 9123

ORIGINATOR FILL IN DATE AND TIME DATE TIME GCT

ON OUTGOING DISPATCHES PLEASE LEAVE ABOUT ONE INCH CLEAR SPACE BEFORE BEGINNING TEXT

ACTION
F-0
F-01
F-02
F-015
F-0115
F-05
F-07
F-1
F-11
F-2
F-3A
F-30
F-31
F-32
F-33
F-34
F-35
F-3B
F-36
F-37
IG-00
VCNO

EFFECTIVE 1200Z/20 MAY THERE IS ESTABLISHED THE 10TH FLEET WITH HEADQUARTERS IN THE NAVY DEPARTMENT UNDER DIRECT COMMAND OF COMINCH TO EXERCISE UNITY OF CONTROL OVER U.S. ANTI-SUBMARINE OPERATIONS IN THAT PART OF THE ATLANTIC UNDER U.S. STRATEGIC CONTROL

2. 10TH FLEET FORCES COMPRISE EASTERN GULF CARIBBEAN SEA FRONTIERS PLUS ATLANTIC SECTOR PANAMA SEA FRONTIER AND ANTI-SUBMARINE SUPPORT FORCES COMPOSED OF SURFACE SUBMARINE AND AIR FORCES ASSIGNED

3. 10TH FLEET TASKS ARE 1ST PROTECTION OF ALLIED SHIPPING IN SEA FRONTIERS MENTIONED IN PARAGRAPH 2. 2ND SUPPORT OF ALL OWN AND ALLIED ANTI-SUBMARINE FORCES OPERATING IN ATLANTIC AREAS, 3RD EXERCISE CONTROL OF CONVOYS AND SHIPPING THAT ARE U.S. RESPONSIBILITIES, 4TH CORRELATION OF U.S. ANTI-SUBMARINE TRAINING AND MATERIAL DEVELOPMENT

4. ALL ANTI-SUBMARINE AGENCIES IN COMINCH HEADQUARTERS ARE TRANSFERRED TO 10TH FLEET HEADQUARTERS

5. WRITTEN DIRECTIVE AND OP-PLAN FOLLOW

10th Fleet 41
F36

CONFIDENTIAL

Make original only. Deliver to Code Room Watch Officer in person. (See Art. 76

OPNAV-NCR 16

DECLASSIFIED
Authority NND 968133
By JK NARA Date 11-2-09

Fig. 6. Original TENTH Fleet Establishment Message (FLTCYBERCOM/TENTH Fleet Powerpoint)

This fleet command’s structure and authority enabled it to forge a close relationship between intelligence, research, development and operations in support of the anti-submarine warfare effort in the Atlantic Ocean. Ladislas Farago, in his 1962 book *The Tenth Fleet*, described

[23] VADM Barry McCullough. “U.S. Fleet Cyber Command/U.S. TENTH Fleet,” Powerpoint, 28 January 2010, Ft. Meade, MD: United States Fleet Cyber Command/10th Fleet, Commander, 2.
[24] Naval Message, COMINCH 19 MAY 1943

the idea behind this organization as being "...to harness in a single, small and flexible, essentially intellectual unit of the best of brainpower to aid the combat elements of conventional seapower in their physical struggle with the U-boats--to put teeth into the anti-U-boat campaign by fusing brain and brawn."[25] Today's Fleet Cyber Command/TENTH Fleet is poised to impact warfare in the cyber domain much as the 20th Century TENTH Fleet successfully enabled U.S. anti-submarine operations in the Atlantic. TENTH Fleet will provide worldwide operational support to commanders for cyberspace operations supporting the forces at sea and ashore in the joint and combined operational environments of the future.[26]

Fleet Cyber Command/TENTH Fleet has been charged with multiple complex and varied missions related to cyberspace operations. The Chairman of the Joint Chiefs has referred to cyberspace operations as "the employment of cyber capabilities where the primary purpose is to achieve military objectives or effects in or through cyberspace. Such operations include computer network operations and activities to operations and activities to operate and defend the Global Information Grid."[27, 28] These missions range from the supporting roles that enable operations in the cyber domain to missions that focus on the protection and integrity of our own information and the networks on which it resides and is transferred. The supporting function of intelligence is necessary to enable effective cyberspace operations.

[25] Ladislas Farago. *The Tenth Fleet*. NY: Ivan Obolensky, 1962.

[26] Chief of Naval Operations, to Commander, U.S. Fleet Forces Command and Director of Naval Intelligence , memorandum, 23 July 2009.

[27] VADM Barry McCullough. "U.S. Fleet Cyber Command/TENTH Fleet." Powerpoint, 28 January 2010, Ft. George G. Meade, MD: Fleet Cyber Command/TENTH Fleet, Commander.

[28] Department of Defense, *Management of the Department of Defense Information Enterprise*, Department of Defense Directive (DODD) 8000.01 (Washington, DC: DoD, 10 February 2009), 10. The Global Information Grid (GIG) is defined as the globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

Specifically, signals intelligence (SIGINT) support to cyber operations is achieved through the relationship Fleet Cyber Command has with National Security Agency/Central Security Service (NSA/CSS), as the Navy's Service Cryptologic Component (SCC). Fleet Cyber Command/TENTH Fleet has invested manpower billets in the form of Cryptologic Technician (CT) sailors and Information Warfare Officers into NSA/CSS organizations around the world. The synergy of an integrated national-operational-tactical force focused on delivering usable intelligence to the warfighter and decision maker has historically been possible because of unity of effort across many organizations.

The original TENTH Fleet's development of new operating concepts for anti-submarine warfare achieved the effect of marginalizing the German threat to allied convoys. This significant achievement was enabled by the unity of effort that allowed the Operational Functions of intelligence, C^2, protection, movement/maneuver, fires and logistics operations to become welded and seamless under one commander. The Function of intelligence proved especially integral to defeating the German U-boat threat and provides an example, through lessons learned, for operations in cyberspace today. Since intelligence and operations were seamless, immediate access to all sources of information affecting the prosecution of German submarines in the Atlantic was available. Human intelligence (HUMINT) cultivated from interrogations of captured U-boat crews; signals intelligence based on radio intercepts of submarine communications; and U-boat locations derived from high frequency direction finding (HFDF) collectively aided TENTH Fleet in developing a deep understanding of German U-boat doctrine. This deep understanding was used to develop anti-submarine concepts of operation and assisted in localizing the enemy threat for prosecution by U. S. Navy surface ships. This historical example of an operational commander's staff employing highly trained and educated personnel to process and analyze information gathered by many varied methods and successfully generating operational effects is an example of how today's TENTH Fleet can be successful.

Fleet Cyber Command and TENTH Fleet, while organizationally integrated, have separate missions of providing support and effects at different levels of war. Fleet Cyber Command is the Navy's component supporting CYBERCOM and is responsible for assisting with the planning, execution and integration of joint cyber warfare capabilities into the operational plans of the combatant commanders while directing Navy cyber operations at the operational-strategic level of war. Additionally, Fleet Cyber Command, as the Navy's Service Cryptologic Component, continues the legacy of providing signals intelligence support to the NSA/CSS.[29] In the TENTH Fleet capacity, the Commander is tasked with providing operational support to Navy commanders worldwide at the operational-tactical level of war in the areas of cyber, information and computer network operations, electronic warfare and space.[30] Together, Fleet Cyber Command/TENTH Fleet has been designated the Navy's cyber component and is under operational control (OPCON) to CYBERCOM while the Chief of Naval Operations maintains administrative control (ADCON) of the forces.

To align Navy cyber planning and capabilities with supported combatant commanders and fleet commanders, TENTH Fleet will establish a Maritime Operations Center (MOC) at its headquarters located at Ft. George G. Meade, MD. The purpose of standing up a TENTH Fleet MOC is to support Fleet Cyber Command, combatant commanders and Fleet commanders while integrating with U.S. Strategic Command/CYBERCOM Operations

[29] Commander, Fleet Cyber Command to Fleet Cyber Command forces, message 291700Z JAN 10, 29 January 2010.
[30] Ibid.

Centers.[31] The MOC construct will streamline the operational decision cycle and provide a structure for quickly and effectively establishing support to an operational level commander.[32] Imbedding TENTH Fleet liaison officers (LNOs) into each MOC in order to ensure mutual understanding and unity of effort will aid in reducing friction and fog between the multiple commands conducting cyber operations. The use of LNOs will be just one more action to ensure the "seams" between intelligence, information operations and space are welded to support operational planning of Navy support to the combatant commanders.

Unity of Effort Through Unity of Command

Dr. Milan Vego refers to the concept of jointness as "...contributing to unity of effort by focusing all the energy of individual services and the armed forces as a whole across the full range of military operations, at all levels of war and in every environment—peace, crisis, and war—toward enhancing the effectiveness of military operations."[33] Unity of effort is ensured by unity of command across the DoD organizations tasked with cyber missions. Keys to achieving this unity is through clearly articulated intentions and objectives by the Commander of CYBERCOM to supporting commanders; Fleet Cyber Command providing advanced cyber-related education to its personnel; the development and assured understanding of cyber doctrine; and fostering an environment of trust at all levels of command.

Developing a process, not just a system, to command and control the cyber forces is also essential to assuring unity of effort through unity of command. The process of

[31] Commander, Fleet Cyber Command to Fleet Cyber Command forces, message 290007Z DEC 09, 29 December 2009.

[32] Chief of Naval Operations, *Maritime Operations Center*, Navy Tactics, Techniques, and Procedures (NTTP) 3-32.1 (Washington, DC: Department of the Navy, CNO, October 2008).

[33] Michael C. Vitale, "Jointness by Design, Not Accident," *Joint Force Quarterly* 3 (Autumn 1995), p. 27, quoted in Milan N. Vego, *Joint Operational Warfare: Theory and Practice* (Newport, RI: U. S. Naval War College, 2009), III-44.

command and control (C^2) refers the individual, but interrelated, functions of "command" and "control". Command is the authority that a commander exercises over subordinates while using available resources in accomplishing assigned missions[34] while control is how the commander implements his directives and establishes limits, focuses efforts, and provides a command structure.[35] Key to enabling successful command and control are the tenants of centralized direction and decentralized execution. Centralized direction ensures unity of effort through unity of command, aids decision making, empowers economy of force, eliminates uncertainty and maximizes control.[36] The assignment of one commander, "dual-hatted" as Fleet Cyber Command and TENTH Fleet, to oversee the operational-strategic and operational-tactical missions of Navy cyber forces ensures unity of effort through centralized direction. Equally as important to effective C^2 is the tenant of decentralized execution which allows for the delegation of authority to subordinate commanders.[37] In layman's terms, decentralized execution is the capacity for a subordinate who has been delegated authority to accomplish the commander's objectives with freedom of action. This tenant commends a trust the commander has bestowed in a subordinate to act with good judgment and skill. The following paragraph provides a historical example of how unity of effort was achieved by applying the tenants of command and control during the Battle of Trafalgar.

The British fleet in the Battle at Trafalgar is an example of centralized command and decentralized execution. Admiral Lord Nelson's victory over the combined fleets of the Spanish and French navies was made possible by his clear command intent, competence

[34] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, as amended through 31 October 2009), 101.

[35] Milan N. Vego, *Joint Operational Warfare: Theory and Practice*, X-19.

[36] Milan N Vego. "Operational Command and Control in the Information Age." *Joint Force Quarterly* , 01 January 2004, 100-107. http://www.proquest.com/ (accessed 21 February 2010).

[37] Chairman, U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms*, Joint Publication (JP) 1-02 (Washington, DC: CJCS, as amended through 31 October 2009), 145.

among his fleet's captains, a deep understanding of the battlespace, and trust among the leaders (captains) in his fleet. The tactics which the British would employ against the superior enemy force were repeatedly discussed and practiced during the months spent searching for the enemy fleet. So, by the time the battle arrived each ship knew precisely their place in formation and the tactics to be executed. Equally important was Lord Nelson's reliance and trust in his captains' judgment and initiative to react in accordance with his guidance even during battle's unpredictable circumstances.[38]

Just as was the case with Lord Nelson's Fleet at the Battle of Trafalgar, Fleet Cyber Command/TENTH Fleet can successfully accomplish each of its diverse and complex missions so long as the commander clearly states his intent; educates his personnel; ensures understanding of a common operational concept and doctrine; and engenders trust at all levels of the organization.

A Counter-Argument: Violating the Simplicity Tenant

Although unity of effort is certainly obtainable through logical command organization and good leadership there does exist the possibility that unity of effort may fall short and become an impediment to effective joint cyber operations. A counter-argument to this paper's thesis is that Fleet Cyber Command/TENTH fleet will fail to achieve unity of effort by violating a basic Operational Command Organization tenant--Simplicity.

The commander of Fleet Cyber Command/TENTH Fleet is tasked with overseeing the Navy's forces and capabilities conducting cyber, information, space and network operations in support of CYBERCOM, the combatant commanders and Fleet commanders.

[38] Joseph F. Callo, *Legacy of Leadership: Lessons from Admiral Lord Nelson* (Central Point, OR: Hellgate Press, 1999), 110.

Additionally, the commander of Fleet Cyber Command is responsible for providing signals intelligence support to the NSA/CSS in his role as the SCC commander.

According to Dr. Vego, a sound command organization should be simple above all else. Considering the sheer size of Fleet Cyber Command/TENTH Fleet: 14, 000 Sailors and civilians; the myriad and varied missions assigned: cyber, information operations, signals intelligence, computer network operations, electronic warfare and space operations; and the scope of supported commander relationships: CYBERCOM, combatant commanders, Fleet commanders, and tactical units, it appears Fleet Cyber Command/TENTH Fleet is the antithesis of a "simple" command organization and, for this reason, could fail to achieve unity of effort.

Mitigating these complex factors is a clearly delineated chain-of-command with one commander providing unambiguous direction and intent across a well-defined Standing Task Organization (Fig. 7); the establishment of a TENTH Fleet MOC providing support the combatant commanders and Fleet commanders; and the integration of LNOs at each MOC.

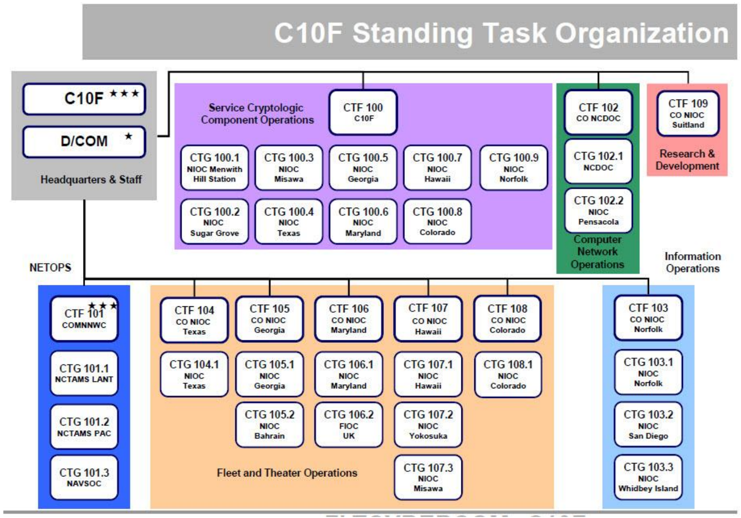


Fig. 7. TENTH Fleet Standing Task Organization

So, while the command organization is large and not simple, Fleet Cyber Command/TENTH Fleet will be successful in achieving unity of effort by fusing Navy's cyber, information operations, cryptologic and space capabilities under the command and control of a single commander.

Recommendations

The Commander of Fleet Cyber Command/TENTH Fleet will best foster unity of effort through following recommendations:

- Invest in the establishment of an advance education program that develops intellectual capital in the cyber force. Partner with civilian academia to expand the opportunities to attain Master- and Doctoral-level degrees in the areas of computer science, electrical and computer engineering, mathematics, and focused regional studies in order to retain a highly skilled workforce.

- Integrate TENTH Fleet liaison officers (LNOs) at each MOC to ensure mutual understanding and unity of effort across supported/supporting commanders.

- Develop an overarching Navy cyber doctrine that nests with Joint cyber doctrine and ensure the Navy's cyber force understands the doctrine conceptually and in practice.

BIBLIOGRAPHY

Anonymous. "Navy Must Think Through Approach To Cyber Domain, CNO Says." *Defense Daily*, 05 February 2010, http://www.proquest.com/ (accessed 17 February, 2010).

Barlow, Jeffrey G. "The Navy's Atlantic War Learning Curve." *Naval History* 22, no. 3 (June 2008): 22-29. http://www.proquest.com/ (accessed 10 February 2010).

Bush, President George W. *Unified Command Plan.* 17 December 2008.

Callo, Joseph F. *Legacy of Leadership: Lessons from Admiral Lord Nelson.* Central Point, OR: Hellgate Press, 1999.

Cebrowski, Arthur D., and Thomas Barnett. "The American Way of War." *Proceedings*, 01 January 2003, 42-43. http://www.proquest.com/ (accessed February 14, 2010).

Chief of Naval Operations. To Director of Naval Intelligence. Memorandum, 26 June 2009.

Chief of Naval Operations. To Commander, U.S. Fleet Forces Command and Director of Naval Intelligence. Memorandum, 23 July 2009.

Commander, Fleet Cyber Command. To Fleet Cyber Command, Message. 291700Z JAN 10. 29 January 2010.

Commander, Fleet Cyber Command. To Fleet Cyber Command, Message. 290007Z DEC 09. 29 December 2009.

Eisenhower, President Dwight D. *Public Papers of the Presidents of the United States: Dwight D. Eisenhower, 03 April 1958.* Washington, DC: Government Printing Office, 1958. http://www.presidency.ucsb.edu/ws/?pid=11340 (accessed 23 March 2010).

Farago, Ladislas. *The Tenth Fleet*. NY: Ivan Obolensky, 1962.

McCullough, VADM Barry. "U.S. Fleet Cyber Command / U. S. Tenth Fleet." Powerpoint. 28 January 2010.

Obama, President Barack. "Remarks on Securing Our Nation's Cyber Infrastructure." 29 May 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/ (accessed 03 February 2010).

Roughead, ADM Gary, Chief of Naval Operations. To Commander, Fleet Forces Command and Director of Naval Intelligence. Memorandum. 23 July 09.

Roughead, ADM Gary, Chief of Naval Operations. Address. Commissioning of United States Fleet Cyber Command and Re-Commissioning of United States Tenth Fleet, Ft. George G. Meade, MD, 29 January 2010.

Secretary of Defense. To secretaries of the military departments. Memorandum, 23 June 2009.

Starling, VADM Denby. "CYBERFOR/NETWARCOM Staff Alignment." Powerpoint. 05 February 2010.

Stavridis, ADM James G., Supreme Allied Commander, Europe. Address. Armed Forces Communications and Electronics Association, San Diego, CA, 02 February 2010.

U.S. Congress. Senate. *U.S. Intelligence Community Annual Threat Assessment: Hearings before the Senate Select Committee on Intelligence.* 111th Cong., 1st sess., 2009.

U.S. Department of Defense. *Management of the Department of Defense Information Enterprise.* Department of Defense Directive (DODD) 8000.01. Washington, DC: DoD, 10 February 2009.

U.S. Federal News Service. "Navy Stands Up Fleet Cyber Command, Reestablishes U.S. 10th Fleet." 30 January 2010. http://www.proquest.com/ (accessed February 13, 2010).

U.S. Marine Corps. "Command and Control: A U.S. Marine Corps Concept Paper." (February 1994). Quoted in Milan N. Vego, *Joint Operational Warfare: Theory and Practice.* Newport, RI: U.S. Naval War College, 2009.

"U.S. Navy Organization and Missions. " *Sea Power* 53, no. 1 (January 2010): 1-9. Military & Government Collection, EBSCOhost (accessed 14 February 2010).

U.S. Navy. To U.S. Fleet, Message, 19 MAY 1943.

U.S. Navy. Office of the Chief of Naval Operations. *Chief of Naval Operations Guidance for 2010.* (September 2009). Washington DC: Department of the Navy, CNO, 2009.

U.S. Navy. Office of the Chief of Naval Operations. *Maritime Operations Center.* Navy Tactics, Techniques, and Procedures (NTTP) 3-32.1. Washington, DC: Department of the Navy, CNO, October 2008.

U.S. Office of the Secretary of Defense. *The Quadrennial Defense Review Report.* Washington, DC: SECDEF, 2010.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Department of Defense Dictionary of Military and Associated Terms.* Joint Publication (JP) 1-02. Washington, DC: CJCS, 31 October 2009.

U.S. Office of the Director of National Intelligence. *The National Intelligence Strategy*, U.S. Government Report. Washington, DC: Director of National Intelligence, August 2009.

Vego, Milan N. *Joint Operational Warfare: Theory and Practice*. 2007. Reprint, Newport, RI: Naval War College, 2009.

Vego, Milan N. "Operational Command and Control in the Information Age." *Joint Force Quarterly* , January 2004. http://www.proquest.com/ (accessed 21 February 2010).

Vitale, Michael C. “Jointness by Design, Not Accident.” *Joint Force Quarterly* 3 (Autumn 1995). Quoted in Milan N. Vego, *Joint Operational Warfare: Theory and Practice.* Newport, RI: U. S. Naval War College, 2009.